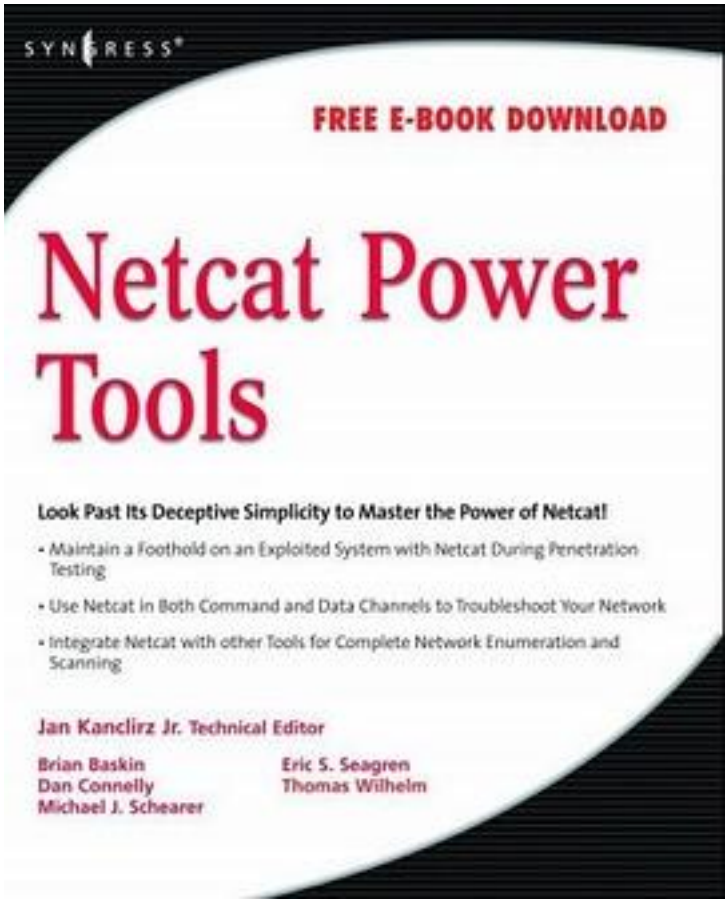
# Netcat Power Tools




Netcat Power Tools_下载链接1_

著者:Jan Kanclirz

出版者:Syngress

出版时间:2008-6

装帧:Paperback

isbn:9781597492577

Originally released in 1996, Netcat is a netowrking program designed to read and write data across both Transmission Control Protocol TCP and User Datagram Protocol (UDP) connections using the TCP/Internet Protocol (IP) protocol suite. Netcat is often referred to as a "Swiss Army knife" utility, and for good reason. Just like the

multi-function usefullness of the venerable Swiss Army pocket knife, Netcat's functionality is helpful as both a standalone program and a backe-end tool in a wide range of applications. Some of the many uses of Netcat include port scanning, transferring files, grabbing banners, port listening and redirection, and more nefariously, a backdoor. This is the only book dedicated to comprehensive coverage of the tool's many features, and by the end of this book, you'll discover how Netcat can be one of the most valuable tools in your arsenal.

* Get Up and Running with Netcat Simple yet powerful...Don't let the trouble-free installation and the easy command line belie the fact that Netcat is indeed a potent and powerful program.

* Go PenTesting with Netcat Master Netcat's port scanning and service identification capabilities as well as obtaining Web server application information. Test and verify outbound firewall rules and avoid detection by using antivirus software and the Window Firewall. Also, create a backdoor using Netcat.

* Conduct Enumeration and Scanning with Netcat, Nmap, and More! Netcat's not the only game in town...Learn the process of network of enumeration and scanning, and see how Netcat along with other tools such as Nmap and Scanrand can be used to thoroughly identify all of the assets on your network.

* Banner Grabbing with Netcat Banner grabbing is a simple yet highly effective method of gathering information about a remote target, and can be performed with relative ease with the Netcat utility.

* Explore the Dark Side of Netcat See the various ways Netcat has been used to provide malicious, unauthorized access to their targets. By walking through these methods used to set up backdoor access and circumvent protection mechanisms through the use of Netcat, we can understand how malicious hackers obtain and maintain illegal access. Embrace the dark side of Netcat, so that you may do good deeds later.

* Transfer Files Using Netcat The flexability and simple operation allows Netcat to fill a niche when it comes to moving a file or files in a quick and easy fashion. Encryption is provided via several different avenues including integrated support on some of the more modern Netcat variants, tunneling via third-party tools, or operating system integrated IPsec policies.

* Troubleshoot Your Network with Netcat Examine remote systems using Netat's scanning ability. Test open ports to see if they really are active and see what protocls are on those ports. Communicate with different applications to determine what problems might exist, and gain insight into how to solve these problems.

* Sniff Traffic within a System Use Netcat as a sniffer within a system to collect incoming and outgoing data. Set up Netcat to listen at ports higher than 1023 (the well-known ports), so you can use Netcat even as a normal user.

* Comprehensive introduction to the #4 most popular open source security tool

available

* Tips and tricks on the legitimate uses of Netcat

* Detailed information on its nefarious purposes

* Demystifies security issues surrounding Netcat

* Case studies featuring dozens of ways to use Netcat in daily tasks

作者介绍:

Jan Kanclirz Jr. (CCIE #12136-Security, CCSP, CCNP, CCIP, CCNA, CCDA, INFOSEC Professional, Cisco WLAN Support/Design Specialist) is currently a Senior Network Information Security Architect at IBM Global Services. Jan specializes in multi vendor designs and post-sale implementations for several technologies such as VPNs, IPS/IDS, LAN/WAN, firewalls, content networking, wireless and VoIP. Beyond network designs and engineering Jans background includes extensive experience with open source applications and Linux. Jan has contributed to several Syngress book titles: Managing and Securing Cisco SWAN, Practical VoIP Security and How to Cheat at Securing a Wireless Network.

In addition to Jans full-time position at IBM G.S., Jan runs a security portal www.MakeSecure.com, where he dedicates his time to security awareness and consulting. Jan lives in Colorado, where he enjoys outdoor adventures.

目录:



## 标签

网络

计算机

网络安全

TCP/IP

Networking

## 评论

---
Netcat Power Tools_下载链接1_

# 书评

---
Netcat Power Tools_下载链接1_